1 билет 31

Определение

Для $n \in \mathbb{N} \quad \sigma(n)$ — сумма натуральных делителей n.

Теорема 24

Если $n = p_1^{k_1} \dots p_s^{k_s}$, *то* $\sigma(n) = \frac{p_1^{k_1+1}-1}{p_1-1} \dots \frac{p_s^{k_s+1}-1}{p_s-1}$.

Доказательство. • Пусть $n_r = p_1^{k_1} \dots p_r^{k_r}$.

• Докажем индукцией по r, что $\sigma(n_r) = \frac{p_1^{k_1+1}-1}{p_1-1} \dots \frac{p_r^{k_r+1}-1}{p_r-1}$.

База для $r = 1$: делители $p_1^{k_1}$ — это $1, p_1, \dots, p_1^{k_1}$ и по формуле суммы геометрической прогрессии их сумма равна $\frac{p_1^{k_1+1}-1}{p_1-1}$.

Переход $r \to r+1$. Так как $(n_r, p_{r+1}^{k_{r+1}}) = 1$, а по Теореме 23 функция $\sigma(n) = \sum_{d \mid n} d$ мультипликативна,

$$\sigma(n_{r+1}) = \sigma(n_r p_{r+1}^{k_{r+1}}) = \sigma(n_r)\sigma(p_{r+1}^{k_{r+1}}) = \left(\frac{p_1^{k_1+1}-1}{p_1-1} \dots \frac{p_r^{k_r+1}-1}{p_r-1}\right)\frac{p_{r+1}^{k_{r+1}+1}-1}{p_{r+1}-1}. \qquad \square$$

2 билет 32

Первообразные корни из 1 в $\mathbb{C}$

Определение

Пусть $n \in \mathbb{N}$. Число $\varepsilon \in \mathbb{C}$ такое, что $\varepsilon^n = 1$, но $\varepsilon^k \neq 1$ при натуральных $k < n$ называется *первообразным корнем из* 1 степени n.

• Пусть $\varepsilon_0, \ldots, \varepsilon_{n-1}$ — все корни степени n из 1, $\varepsilon_k = (\cos(\frac{2\pi k}{n}), \sin(\frac{2\pi k}{n}))$.

Теорема 25

1) *Существует в точности $\varphi(n)$ первообразных корней степени n из 1, это в точности такие корни ε_j, что $(j, n) = 1$.*
2) *Если ε_j — первообразный корень степени n из 1, то ε_j, ε_j^2, $\ldots$, ε_j^n — все корни степени n из 1.*

Доказательство. • По формуле Муавра, $\arg(\varepsilon_j^k) = \frac{2\pi kj}{n}$. Разберем два случая.

Случай 1: $(j, n) = d > 1$.

• Тогда $m = \frac{n}{d} \in \mathbb{N}$, $m < n$ и $y = \frac{j}{d} \in \mathbb{Z}$.

• Следовательно, $\arg(\varepsilon_j^m) = \frac{2\pi mdy}{md} = 2\pi y$ и $\varepsilon_j^m = 1$. Это означает, что ε_j не является первообразным корнем из 1 степени n.

Случай 2: $(j, n) = 1$.

• Тогда аргументы $\varepsilon_j, \varepsilon_j^2, \ldots, \varepsilon_j^{n-1}, \varepsilon_j^n$ — это $\frac{2\pi j}{n}$, $\ldots$, $\frac{2\pi nj}{n}$.

• По Теореме 13, числа j, $2j$, $\ldots$, nj — ПСВ $\pmod{n}$. Значит, среди их остатков от деления на n каждый встречается ровно один раз.

• Тогда $\frac{2\pi \cdot j}{n}$, $\frac{2\pi \cdot 2j}{n}$, $\ldots$, $\frac{2\pi \cdot nj}{n}$ — это в точности такие аргументы, как $\frac{2\pi}{n}$, $\frac{4\pi}{n}$, $\ldots$, $\frac{2n\pi}{n}$ (напомним, что аргумент не меняется при прибавлении 2π).

• Это означает, что $\varepsilon_j, \varepsilon_j^2, \ldots, \varepsilon_j^{n-1}, \varepsilon_j^n$ — это в точности ε_0, $\ldots$, ε_{n-1} — все корни степени n из 1.

• Понятно, что $\varepsilon_j^n = 1$, значит, в меньших степенях ε_j не равен 1, то есть, это первообразный корень степени n из 1. $\square$